



Fraud Newsletter

April 2008

Sheriff Steve Mansfield

Fraud and ID Theft Information – To Better Protect the Residents of Lewis County

"If it's too good to be true it normally is"

Fraud is simply a theft by trick. It can take the form of chain letters claiming huge amounts of cash to those who send money in or people claiming they will provide a service and never do.

Identity theft and identity fraud are terms used to refer to all types of crimes in which someone wrongfully obtains and uses another person's personal data in a way that involves fraud or deception for economic gain. This newsletter is intended to keep the public informed of the most recent fraud schemes happening in our county. It will also provide resources to help you take precautions to protect yourself from these vicious crimes.

PROTECT YOUR ID

- 1** Always know who you are providing personal information to
- 2** If you use passwords to access accounts make sure to change them often
- 3** Never provide personal information in response to any unsolicited offer
- 4** Know the company you are dealing with when making online purchases

Current Scams and Frauds Hitting Lewis County

Phishing Attacks

This is again the season for Phishing Scams. They all start out the same way with an email from a financial company advising there is a problem with your account. In the email you are directed by a link to a website to fix the problem. This follows the normal old phishing scam with both the email and link being false. If you click on the link, you find yourself at a web page that looks official and requests your account information. This is just an attempt to steal your account information and your money. The key to these cases is the email is not individually addressed. Also, banks and credit unions do not notify customers by email of problems with their accounts. Victims of this scam should contact their bank or credit union immediately!

Because of the continued risk of these scams to our community we have again posted ways to protect yourself on page 2.

Ways to Protect Against Identity Thefts

1. **Guard your information, online and offline.** While news headlines make identity theft seem like it's mainly an online issue, you should recognize that there are also very real offline dangers.
 - **Trash doesn't always end up in the dump.** A recent study suggests that you are in greater danger from identity thieves rummaging for important papers in your trash or breaking into your mailbox than from online theft.
 - **Stolen wallets can become stolen identities.** It's estimated that 14% of identity thefts are a result of stolen wallets, checkbooks, and credit cards.
 - **Offline precautions.** To protect yourself, consider shredding documents containing your personal information, such as account statements, locking your mailbox, and emptying your wallet of anything you don't absolutely have to carry.
2. **Don't respond to email or phone calls asking for your account information.**
 - **Phishing emails.** Phishing (fake) emails are made to look like they're from legitimate companies, but are actually from identity thieves. These emails warn you of account problems or other urgent issues in order to trick you into clicking through to a spoof website or calling a fake customer service number.
 - **Phone Calls.** Beware of unsolicited phone calls claiming to be from customer service centers requesting that you provide sensitive personal information. You should hang up and call the number on the company's website.
3. **Protect your computer.**
 - **Software protection.** The key to securing your computer is to use protective software and keep it up to date. Make sure you install all security patches available from the developer of your operating system. Run antivirus software to check incoming emails and update virus definitions frequently. Set up a firewall to prevent intruders from getting into your network or computer.
 - **Password protection.** Always choose strong passwords to protect accounts. Mix upper and lowercase letters. Use symbol characters. Create unique passwords for each one of your accounts.
4. **Stay alert.**
 - **Act quickly.** The longer a breach goes undiscovered, the more costly it becomes.
 - **Monitor your accounts frequently.** Check your credit card activity and bank balances often to look for suspicious activity.

Information borrowed from several sources



The internet is a powerful tool used by both legitimate businesses and scam artists alike. Always take steps to protect yourself and your personal information as you would protect your home or car.

Who should I notify about a fraud or scam attempt?

- Federal Trade Commission toll free hotline: 877-FTC-HELP (877-382-4357)
- Federal Trade Commission on-line complaint form (www.ftc.gov)
- Internet Fraud Complaint Center (www.ic3.gov/)
- Lewis County Sheriff's Office – 360-740-1329

Other Resources

Phone Busters (Canadian Link) - <http://www.phonebusters.com/>

The Federal Citizen Information Center -
<http://www.pueblo.gsa.gov/scamsdesc.htm>

The Federal Trade Commission - <http://www.consumer.gov/idtheft/>

The FBI Fraud Information page -
<http://www.fbi.gov/majcases/fraud/fraudschemes.htm>

Lewis County Sheriff's Office Mission Statement

To make a positive difference for members of our community by seeking and finding ways to affirmatively promote, preserve and deliver a feeling of security, safety and quality service.



Sheriff Steve Mansfield

Committed to make a difference.